



DEPARTMENT OF JUSTICE

[CPCLO Order No. 001-2023]

Privacy Act of 1974; System of Records

AGENCY: Office of Privacy and Civil Liberties, United States Department of Justice.

ACTION: Notice of a new system of records.

SUMMARY: Pursuant to the Privacy Act of 1974 and Office of Management and Budget (OMB) Circular No. A-108, notice is hereby given that the Office of Privacy and Civil Liberties (hereinafter OPCL), a component within the United States Department of Justice (DOJ or Department), proposes to develop a new system of records titled Data Protection Review Court Records System, JUSTICE/OPCL-001. The OPCL proposes to establish this system of records to maintain records of matters reviewed by and decisions made by the Data Protection Review Court (DPRC) concerning determinations made by the Civil Liberties Protection Officer of the Office of the Director of National Intelligence in response to complaints that allege certain violations of United States law in the conduct of United States signals intelligence activities.

DATES: In accordance with 5 U.S.C. 552a(e)(4) and (11), this notice is effective upon publication, subject to a 30-day period in which to comment on the routine uses, described below. Please submit any comments by [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: The public, OMB, and Congress are invited to submit any comments by mail to the United States Department of Justice, Office of Privacy and Civil Liberties, ATTN: Privacy Analyst, Two Constitution Square, 145 N St., NE, Suite 8W-300,

Washington, DC 20530; by facsimile at 202-307-0693; or by email at privacy.compliance@usdoj.gov. To ensure proper handling, please reference the above CPCLO Order No. on your correspondence.

FOR FURTHER INFORMATION CONTACT: Katherine Harman-Stokes, Director (Acting), Office of Privacy and Civil Liberties, U.S. Department of Justice, Two Constitution Square, 145 N St., NE, Suite 8W-300, Washington, DC 20530; email, privacy.compliance@usdoj.gov; telephone: (202) 514-0208; facsimile (202) 307-0693.

SUPPLEMENTARY INFORMATION:

On October 7, 2022, the President of the United States issued Executive Order (E.O.) 14086, Enhancing Safeguards for United States Signals Intelligence Activities, 87 FR 62283 (Oct. 14, 2022), which directed the Attorney General to establish the DPRC as the second level of a two-level redress mechanism for alleged violations of law regarding signals intelligence activities. The Attorney General issued a regulation on October 7, 2022, now at 28 CFR 201, “Data Protection Review Court.” 87 FR 628303 (Oct. 14, 2022).

The redress mechanism will provide for the review of complaints submitted by individuals through their designated public authorities in designated countries and regional economic integration organizations, alleging certain violations of United States law concerning United States signals intelligence activities covered in E.O. 14086 (“covered violation”). The E.O. 14086 implements commitments made by the United States as part of the EU-U.S. Data Privacy Framework announced in March 2022 to foster trans-Atlantic data flows.

The first level of the new redress mechanism established by E.O. 14086 is the investigation and review of complaints by the Office of the Director of National

Intelligence Civil Liberties Protection Officer (ODNI CLPO). The ODNI CLPO will conduct an initial review of the complaint to assess whether it meets the requirements necessary for a redress review pursuant to E.O. 14086, i.e., whether the complaint is a “qualifying complaint.” Upon confirming a complaint is qualified, the ODNI CPLO will determine whether a covered violation occurred, and, where necessary, the appropriate remediation. As a second level, the complainant or an element of the Intelligence Community, as defined in E.O. 14086 section 4(g), may seek review by the DPRC of the ODNI CLPO’s determination.

The DPRC has been established within the Department, it and will consist of individuals chosen as judges and “special advocates” from outside the Executive Branch of the United States Government to provide independent and impartial adjudication of applications for review of determinations of the ONDI CLPO described above.

Exercising the Attorney General’s delegated authority under 28 U.S.C. 511 and 512 to provide advice and opinion on questions of law, as well as the authority of the DPRC under EO 14086, the DPRC will review whether the ODNI CLPO’s determination regarding the occurrence of a covered violation was legally correct and supported by substantial evidence and whether, in the event of a covered violation, the ODNI CLPO’s determination as to the appropriate remediation was consistent with E.O. 14086 or other applicable laws. Each application will be reviewed by a three-judge panel of the DPRC convened by the Department’s Office of Privacy and Civil Liberties (OPCL), which will provide administrative support to the DPRC.

The regulations require the DPRC and OPCL, in support of the DPRC, to maintain records of the DPRC’s activities. For each application for review, OPCL will maintain all records pertaining to the DPRC’s review, including submissions from the

complainant, the Special Advocate, or an element of the intelligence community. 28 CFR 201.9(j), *see also* 28 CFR 201.5, et seq.

Pursuant to 28 CFR 201.9(i), certain classified information in the system indicating a violation of any authority subject to the oversight of the Foreign Intelligence Surveillance Court (“FISC”) will be shared with the Assistant Attorney General for National Security, who shall report violations to the FISC as required by law and in accordance with its rules of procedure. Similarly, information in the system will be accessible to the Privacy and Civil Liberties Oversight Board (“PCLOB”) as necessary to conduct the annual review of the redress process described in section 3(e) of E.O. 14086, consistent with the protection of intelligence sources and methods.

In accordance with 5 U.S.C. 552a(r), the Department has provided a report to OMB and Congress on this new system of records.

Dated: May 10, 2023.

Peter A. Winn,
Chief Privacy and Civil Liberties Officer (Acting),
United States Department of Justice.

JUSTICE/OPCL-001

SYSTEM NAME AND NUMBER:

Data Protection Review Court Records System, JUSTICE/OPCL-001.

SECURITY CLASSIFICATION:

The majority of information in this system of records is classified. The remaining information is sensitive but unclassified.

SYSTEM LOCATION:

United States Department of Justice, 950 Pennsylvania Ave., NW., Washington, DC 20530-0001.

SYSTEM MANAGER(S):

Director, Office of Privacy and Civil Liberties, U.S. Department of Justice, Two Constitution Square, 145 N St., NE, Suite 8W-300, Washington, DC 20530; email, privacy.compliance@usdoj.gov; telephone: (202) 514-0208; facsimile (202) 307-0693.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Authority for maintaining this system exists under 5 U.S.C. 301; 28 U.S.C. 509, 510-512; 28 CFR 0.72; 28 CFR part 201; Executive Order 14086 and other applicable executive order(s) governing foreign intelligence surveillance and classified national security information.

PURPOSE(S) OF THE SYSTEM:

The purpose of the system is to maintain records of the information received, reviewed, or created by the DPRC for each application for review and decision of a DPRC panel handling a specific matter; to make records available for consideration as non-binding precedent to future panels of the DPRC; to provide reports, when appropriate, to the Assistant Attorney General for National Security, other relevant DOJ officials, and members of the Intelligence Community; for related litigation, if applicable; to provide information to the PCLOB as necessary to conduct the annual review of the redress process described in section 3(e) of E.O. 14086; for DPRC personnel, and OPCL personnel supporting the DPRC, to prepare, process and track applications for review and perform other functions as needed.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individual complainants seeking review pursuant to E.O. 14086 and Department of Justice regulation 28 CFR 201 of an Office of the Director of National Intelligence Civil Liberties Protection Officer (ODNI CLPO) determination in response to qualifying complaints; individuals who did not submit a qualifying complaint but who are identified in connection with the qualifying complaint, including for example, the individual complainant's counsel, if any, and personnel with the public authority of a designated state; members of the United States Government workforce, including personnel of elements of the Intelligence Community involved in investigating and reviewing complaints or involved in signals intelligence activities related to a complaint, and individuals serving as Judges on the DPRC or Special Advocates.

CATEGORIES OF RECORDS IN THE SYSTEM:

The system consists of all records relating to applications for review of an ODNI CLPO determination in response to complaints submitted through the redress mechanism established pursuant to section 3 of E.O. 14086; including all information received,

reviewed, and created by the DPRC in the adjudication of an application for review; the decisions of the DPRC; and records created and maintained for administrative or operational purposes for the DPRC. This also includes the records received from, generated by, or about, ODNI CLPO, elements of the Intelligence Community, the complainant and counsel through the public authority of a qualifying state, and from the Special Advocates. The records in this system also include communications between ODNI CLPO, DPRC Judges and Special Advocates, PCLOB, public authority in the designated country or regional economic integration organization, the complainant, and OPCL personnel supporting the DPRC. The system will also contain records related to the appointment of DPRC Judges and Special Advocates, DPRC's rules of procedures and processes for filing an application for review, and other administrative or operational records.

RECORD SOURCE CATEGORIES:

The system contains records that originated from Department of Justice personnel involved in the administration of the DPRC and the implementation and execution of the two-level redress mechanism described in E.O. 14086, and records originating from ODNI, PCLOB, elements of the Intelligence Community, the complainant and counsel, DPRC Judges and Special Advocates, and the public authority of a designated country or regional economic integration organization.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b), all or a portion of the records or information contained in this system of records may be disclosed for the purposes described below, to the extent such disclosures are compatible with the purposes for which the information was collected:

- A. To any person or entity that the Department has reason to believe possesses information regarding a matter within the jurisdiction of the DPRC, to the extent deemed to be necessary by the DPRC or OPCL in order to elicit such information or cooperation from the recipient for use in the performance of an authorized activity.
- B. Where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law – criminal, civil, or regulatory in nature – the relevant records may be referred to the appropriate Federal, State, local, Territorial, Tribal, or foreign law enforcement authority or other appropriate entity charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law.
- C. In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body, when the Department determines that the records are relevant to the proceeding in accordance with applicable laws, rules, and Department policies.
- D. To the news media and the public, including disclosures pursuant to 28 CFR 50.2, unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy, with the concurrence of the Department's Chief Privacy and Civil Liberties Officer.
- E. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records.

- F. To a former employee of the Department for purposes of: responding to an official inquiry by a Federal, State, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.
- G. To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record, whether the individual is residing in the United States or abroad at the time of the request.
- H. To the National Archives and Records Administration for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.
- I. To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that there has been a breach of the system of records; (2) the Department has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the Department (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.
- J. To another Federal agency or entity, when the Department determines that information from this system of records is reasonably necessary to assist the

recipient agency or entity in (1) responding to a suspected or confirmed breach, or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

K. To any agency, organization, or individual for the purpose of performing authorized audit or oversight operations of the DPRC or OPCL and meeting related reporting requirements.

L. To such recipients and under such circumstances and procedures as are mandated by Federal statute or treaty.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records in this system are stored on paper and/or in electronic form. Records are stored securely in accordance with applicable laws, regulations, and policies. Records that contain classified national security information are stored in accordance with applicable executive orders, statutes, and agency implementing regulations.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Information is retrieved by the unique case number assigned to the application for review, the name of the complainant, the public authority that submitted the complaint for the complainant, or the designated country or regional economic integration organization.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records in this system are maintained and disposed of in accordance with all applicable statutory and regulatory requirements.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Information in this system in electronic or hard copy form is subject to administrative, technical, and physical safeguards in accordance with applicable laws, rules, and policies, including the Department's automated systems security and access policies. Classified information is appropriately stored in safes and on secure servers in accordance with other applicable requirements. Records and technical equipment are maintained in a secured area with restricted access. Internet connections are protected by multiple firewalls and data is encrypted in accordance with applicable laws, rules, and Department policies. Security personnel conduct periodic vulnerability scans using DOJ-approved software to ensure security compliance and security logs are enabled for computers to assist in troubleshooting and forensics analysis during incident investigations. Users of individual computers can only gain access to data through a multi-factor authentication process; direct access to certain information is restricted depending on a user's role and responsibility within the organization and system.

RECORD ACCESS PROCEDURES:

A major part of this system is exempted from this requirement; specifically, this system is exempt from Privacy Act subsections (c)(3) and (4); (d); (e)(1), (2), (3), (4)(G), (H) and (I), (5) and (8); (f); (g); and (h) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2), (k)(1), (2), and (5). An individual who is the subject of a record in this system of records may access those records that are not exempt from access. A determination as to exemption shall be made at the time a request for access is received. A request for access to records contained in this system shall be made in writing and clearly marked "Privacy Act Access Request." The request should include the full name of the individual

involved, the individual's current address, date and place of birth, and their signature which shall be notarized or made pursuant to 28 U.S.C. 1746 as an unsworn declaration. The request must describe the records sought in sufficient detail to enable Department personnel to locate them with a reasonable amount of effort. Requests should be directed to the Office of Information Policy. *See <https://www.justice.gov/oip/make-foia-request-doj>.*

Although no specific form is required, you may obtain forms for this purpose from the FOIA/Privacy Act Mail Referral Unit, United States Department of Justice, 950 Pennsylvania Avenue NW, Washington, DC 20530, or on the Department of Justice web site at <https://www.justice.gov/oip/oip-request.html>.

More information regarding the Department's procedures for accessing records in accordance with the Privacy Act can be found at 28 CFR part 16 subpart D, "Protection of Privacy and Access to Individual Records Under the Privacy Act of 1974."

CONTESTING RECORD PROCEDURES:

Individuals seeking to contest or amend records maintained in this system of records must direct their requests to the address indicated in the "RECORD ACCESS PROCEDURES" section, above. All requests to contest or amend records must be in writing and clearly marked "Privacy Act Amendment Request." All requests must state clearly and concisely what record is being contested, the reasons for contesting it, and the proposed amendment to the record. Some information may be exempt from the amendment provisions as described in the "EXEMPTIONS PROMULGATED FOR THE SYSTEM" section, below. An individual who is the subject of a record in this system of records may contest or amend those records that are not exempt. A determination of whether a record is exempt from the amendment provisions will be made after a request is received.

More information regarding the Department's procedures for amending or contesting records in accordance with the Privacy Act can be found at 28 CFR §16.46, "Requests for Amendment or Correction of Records."

NOTIFICATION PROCEDURES:

Individuals may be notified if a record in this system of records pertains to them when the individuals request information utilizing the same procedures as those identified in the "RECORD ACCESS PROCEDURES" section, above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

The Attorney General has exempted this system from subsections (c)(3) and (4); (d); (e)(1), (2), (3), (4)(G), (H) and (I), (5) and (8); (f); (g); and (h) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2), (k)(1), (2), and (5). Rules are in the process of being promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c) and (e), and are in the process of being published in the *Federal Register*. These exemptions apply only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2), (k)(1), (2) or (5). A determination as to exemption shall be made at the time a request for access or amendment is received.

HISTORY:

None.